Cyber-ranges as cybersecurity training environments

NEOFYTOS GEROSAVVA, PRINCIPAL ANALYST (8BELLS) -SPIDER CONSORTIUM

CYBER RANGE NETWORK JOINT WEBINAR
26/11/2020

What is a cyber range?

"A cyber range is a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organisation's ICT, OT, mobile and physical systems, applications and infrastructures, including the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend upon. ***A cyber range includes a combination of core technologies for the realisation and use of the simulation environment and of additional components which are, in turn, desirable or required for achieving specific cyber range use cases****."*

– European Cyber Security Organisation (ECSO), "Understanding Cyber Ranges from Hype to Reality" (White Paper) rel. 30-March 2020.

Background

- The complex landscape surrounding today's cyber security strengthens the need for better trained and qualified experts securing critical multi-tenant and multi-service environments, such as 5G mobile networks.
- During the last years, the number of cyber-attacks has gradually increased and various recent security incidents worldwide have demonstrated the fact that there is an increase also in the complexity and severity of cyber security threats
- According to 2020 Official Annual Cybercrime Report by Cybersecurity Ventures, sponsored by Herjavec Group, cyberattacks will cost the world $6 trillion annually by 2021, in comparison with the $3 trillion in 2015
- The attackers are becoming more sophisticated and they are using even more advanced methods and techniques.
- As an effect companies worldwide understand the importance of finding new ways,approaches and innovative cyber security models to keep their assets and their infrastructures safe

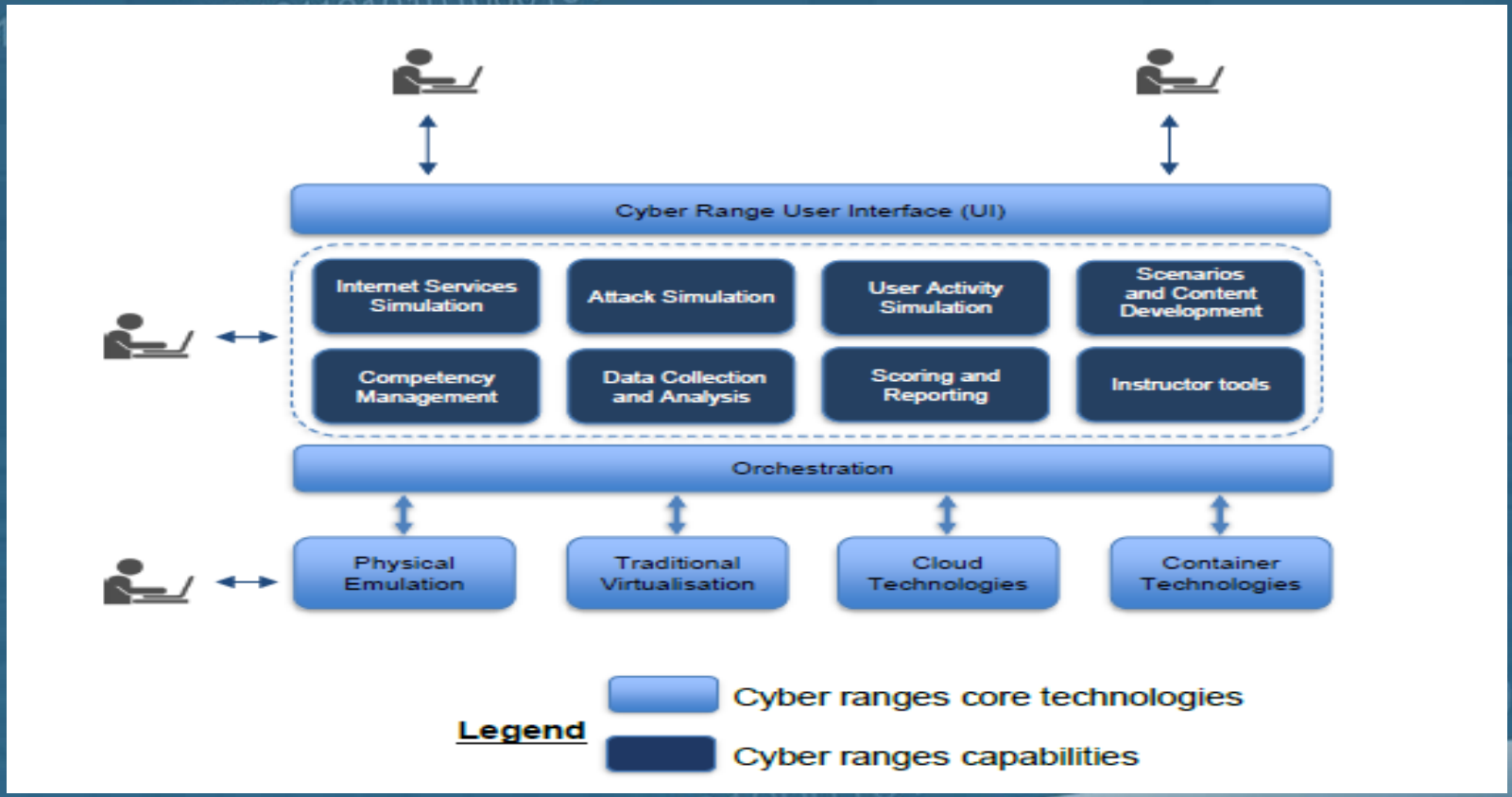
The Cyber ranges concept

- Traditionally, cyber ranges were platforms that enabled commercial companies, government agencies and military organizations to study the effectiveness of their cybersecurity technologies
- These platforms can provide the chance to their potential users to simulate real-world complexity cyber scenarios with high fidelity and train employees and customers on the latest threats through high quality realistic cyber exercises, without endangering the productive environment, which is just replicated virtually.
- A cyber range provides a place to practice correct and timely responses to cyber attacks and the participants can practice skills such as network defense, attack detection and mitigation, penetration testing etc
- At a high level, the two key drivers responsible for the growing demand for cyber ranges are the cementing of cyber as a separate domain of warfare and the development and wide spreading of cloud technology, acting as a major enabler for cyber ranges to develop.

Benefits of Cyber Range Solutions

- Providing the experience of real-world threats /cyberattacks in a safe and well controlled environment
- Because of their ability to represent real-world cyber threat scenarios in a virtual environment, they also present an opportunity to enhance organizational training capabilities
- Provide the opportunity to various type of organizations to test their infrastructures and identify and assess potential vulnerabilities.
- Software developers can use cyber range applications to validate virtual Proof of Concepts.
- Cyber ranges come equipped with sets of gamified elements providing all potential benefits of gamification in learning
- Offer a simulated environment with real time feedback where teams can work and train together to improve their capabilities
- An efficient way for trainees to gain practical knowledge through hands on activities
- By facilitating high-fidelity simulations, they can improve stability, security and performance of cyberinfrastructures

Cyber Range Functionalities

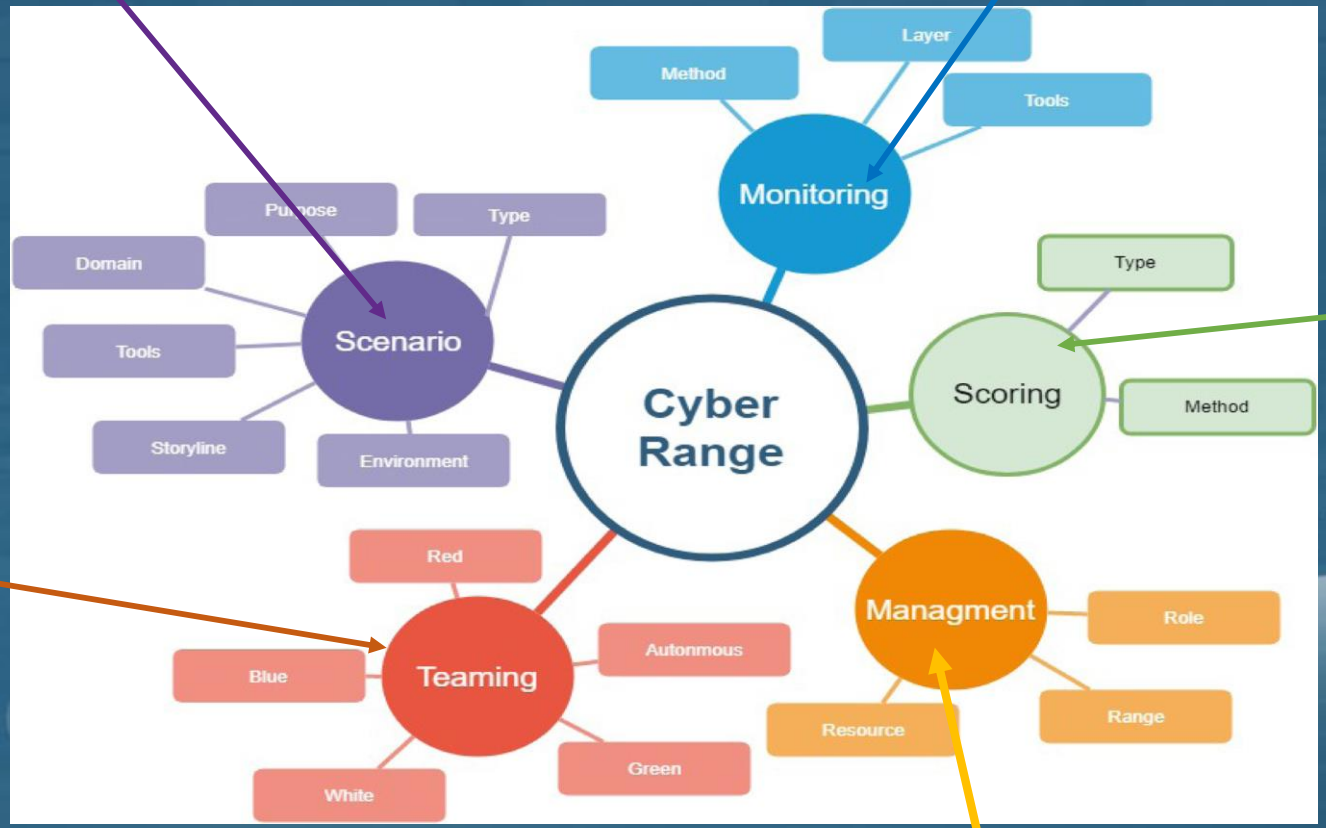


By definition, a cyber range does not need to include all or any of the scheme capabilities. The difference between cyber ranges lies primarily in the amount of work required for each cyber range to deliver specific use cases..

TAXONOMY

Scenarios define the execution environment as well as the storyline that indicates the execution steps of a test or a training exercise.

Monitoring includes the methods, the tools and the layers at which real time monitoring of cyber security exercises and tests are performed



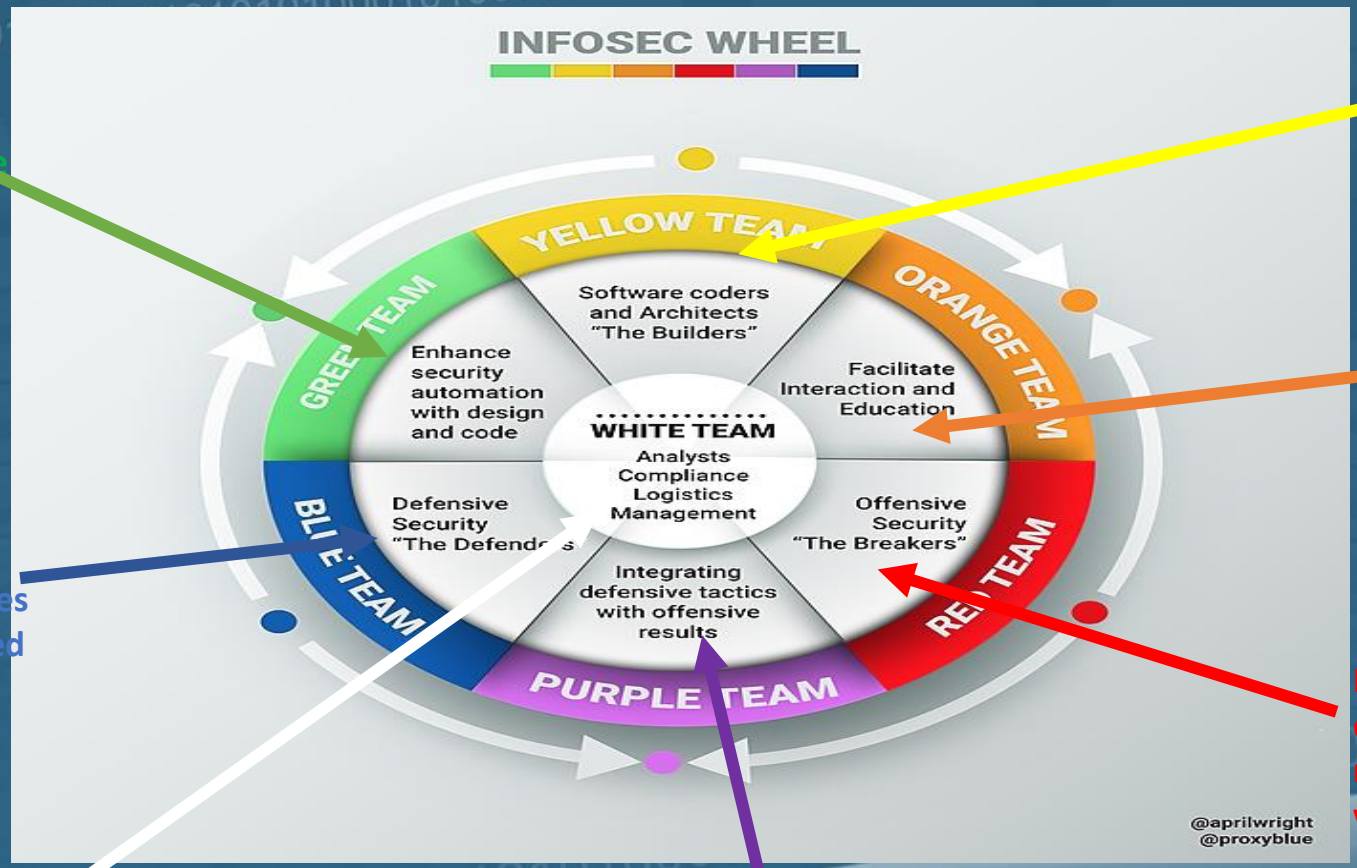
Teaming includes an individual and a group of individuals that design, develop, manage and participate in a cyber security exercise or a test

Scoring uses data from monitoring systems in order to give performance related semantics to the low level technical events observed during monitoring of cyber security exercises and tests.

Management involves the assignment of roles and duties to individuals and team

TEAMING

Green team is responsible for the development, monitoring and maintenance of the exercise infrastructure designed by the white team.



Yellow Teams software builders and application developers , generating legitimate network traffic which can be used by red and blue teams in attack and defense.

Orange teams inspire coders and architects to be more security conscious.

Blue team ,threat hunters, responsible to identify and patch potential vulnerabilities that can be exploited by a red team.

Red team – ethical hacking, cyber- security adversaries are modeled to exploit potential vulnerabilities

White team designs the exercise and experiment scenario, objectives, rules and evaluation criteria. They set a set of rules of engagement between red and blue team

Purple teams perform the communication role between multiple exercises teams. They do information sharing to increase the exercise effectiveness and facilitate improvements

Sources

- “2019 Official Annual Cybercrime Report” HERJAVEC GROUP
- “Cyber ranges and security testbeds: Scenarios, functions, tools and architecture "Muhammad Mudassar Yamin, Basel Katt, Vasileios Gkioulos
- CyberSec4Europe D7.1 Report on existing cyber ranges, requirements
- Design of Cyber Warfare Testbed Yogesh Chandra, and Pallaw Kumar Mishra
- Cyber Ranges: The (R)evolution in Cybersecurity Training, Dr. Jorge López Hernández-Ardieta Head of Cybersecurity Solutions & Digital Specialist
- Features and Architecture of The Modern Cyber Range: A Qualitative Analysis and Survey, Ishaani Priyadarshini
- European Cyber Security Organization (ECSO), "Understanding Cyber Ranges from Hype to Reality" (White Paper) rel. 30-March 2020.
- What is a Cyber Range? https://www.cyberwiser.eu/content/what-cyber-range
- Introducing the InfoSec color wheel https://hackernoon.com/introducing-the-infosec-colour-wheel-blending-developers-with-red-and-blue-security-teams-6437c1a07700
- What Is a Cyber Range? https://www.cloudshare.com/virtual-it-labs-glossary/what-is-a-cyber-range

Thank you !


Cyber MAR
FORESIGHT
SPIDER
5G CYBER RANGE
Cyber Range Network
Joint Webinar
26th November 2020
11.00 – 12.50 CET